



State of Michigan
John Engler, Governor

Department of Consumer & Industry Services
Kathleen M. Wilbur, Director

Office of Financial and Insurance Services
Frank M. Fitzgerald, Commissioner

Division of Financial Institutions
P.O. Box 30224
Lansing, MI 48909
Tel. (517) 373-3460
Web site: www.cis.state.mi.us/ofis/

DATE: March 16, 2001

LETTER NO: 2001-CU-04

TO: The Board of Directors and Management
Of Michigan State-Chartered Credit Unions

SUBJECT: Comprehensive Information Security Program

Purpose of this Letter

This letter is to advise credit union officials that all federally insured credit unions will be required to adopt a comprehensive information security program by July 1, 2001. The requirement is a result of the Gramm-Leach-Bliley Act signed into law on November 12, 1999, which impacts the existing regulation governing security programs in federally insured credit unions. Specifically, paragraph (b) of 748.0 NCUA Rules and Regulations will be revised to include security concerns of member information relating to the emerging electronic marketplace. Member information includes any records, data, files, or other information about a member containing nonpublic personal information. This includes records in paper, electronic, or any other form that are within the control of a credit union or that are maintained by any service provider on behalf of a credit union.

Many credit unions have documented information security plans, however examinations reveal that the plans are not maintained, do not address certain aspects of information security, and are not reviewed or approved by the credit union Board on a recurring basis.

Guidelines

Guidelines for a comprehensive information security program include:

- (1) Identification and assessment of risks that may threaten member information
- (2) The development of the written plan containing policies and procedures to manage and control the risks identified
- (3) Implementation and testing of the plan
- (4) Adjusting the plan on a continuing basis to account for changes in technology, the sensitivity of member information, and internal or external threats to information security.

Objectives

Objectives for a comprehensive information security program include establishing appropriate measures to ensure the security and confidentiality of member information, to protect against any anticipated threats or hazards to the security or integrity of such information, and to protect against unauthorized access to or use of member information that could either: (1) result in substantial harm or inconvenience to any member; or (2) present a safety and soundness risk to the credit union.

Responsibility

The Board of Directors is responsible to oversee the efforts to develop, implement, and maintain the program, including the regular review of management reports. They are also responsible to approve the written information security policy and plan. Management's responsibilities include performing an ongoing assessment of changes in technology and the impact on the credit union, as appropriate. Management must also evaluate the impact on the security plan of changing business arrangements (e.g. alliances, joint ventures, or outsourcing arrangements), and changes to member information systems. Management must document compliance with guidelines, and keep the board of directors informed on the current status of the information security program.

Conclusion

Emerging information processing technologies have created new risk and control issues for credit unions. Written policies, procedures, and standards can provide the basis for establishing and maintaining proper control over member information. All Michigan state-chartered credit unions will be required to have a comprehensive information security program in place by July 1, 2001. Attached is a checklist of issues to consider when developing a comprehensive information security program.

Very truly yours,

Frank M. Fitzgerald, Commissioner
Office of Financial and Insurance Services

Consider the following in relation to the sensitivity of information as well as the complexity and scope of your credit union information systems when developing policies and procedures:

- a. access rights to member information
- b. access controls on member information systems, including controls to authenticate and grant access only to authorized individuals and companies
- c. access restrictions at locations containing member information, such as buildings, computer facilities, and records storage facilities
- d. encryption of electronic member information while in transit or in storage on networks or systems to which unauthorized individuals may have access
- e. procedures to confirm that member information system modifications are consistent with the credit union's information security plan
- f. dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information
- g. contract provisions and oversight mechanisms to protect the security of member information maintained or processed by service providers
- h. monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems
- i. response programs that specify actions to be taken when unauthorized access to member information is suspected or detected
- j. protection against destruction of member information due to potential physical hazards, such as fire and water damage
- k. response programs to preserve the integrity and security of member information in the event of computer or other technological failure, including, where appropriate, reconstruction of lost or damaged member information